Title:
Free Access to Information & Secrecy of Data in Montenegro
Law comments with recommendations

Author:
Helen Darbishire
Access Info Europe
Network for the Affirmation of Non-Governmental Sector – MANS

Design & layout:
Dejan Milovac

Printed by:
"Lider" – 069 016 054

Contact details:
Network for the Affirmation of Non-Governmental Sector – MANS
Bohinjska bb, Stari aerodrom, Podgorica, Montenegro
Tel/fax +381.81.652.265
mans@cg.yu, www.mans.cg.yu

FREE ACCESS TO INFORMATION
& SECRECY OF DATA IN MONTENEGRO

Law comments with recommendations

2007

TABLE OF CONTENTS

PART I

LAW ON FREE ACCESS TO INFORMATION

Introduction

The purpose of this analysis and recommendations is to propose ways in which Montenegro's Law on Free Access to Information (LFATI) could be amended to ensure fuller respect for the right of access to information. The LFATI adopted in November 2005 has already proved its value in ensuring that information that was not previously public in Montenegro has entered the public domain. This includes information related to privatization of state companies, and basic budgetary and structural information about the security services.

There are however, a number of provisions of the law that are still unclear, confused or contradictory, and fall short of international standards. These include the provisions on copies and on costs, the need to appoint establishment of information officers in each public body, and the need to clarify and elaborate timeframes. There are also some typical elements of ensuring the right to information that are absent from this law and would greatly enhance its effectiveness, both for requestors and for the administration. These include the duty to assist requestors, the proactive provision of information, greater detail on personal data protection, elaboration of the right to environmental information, and the establishment of an Information Commissioner.

In conducting this analysis, we have been guided by established international standards, including the provisions of the ICCPR and ECHR, and the Recommendation 2002(2) of the Council of Europe on Access to Official Documents. We have also drawn on comparative law and jurisprudence, particularly that from the member countries of the European Union.

International law has clearly established not only a right of access to information but a positive obligation on government to respect that right and take measures to ensure that information is available to the public. The Inter-American Court of Human Rights, ruling in the case of *Claude Reyes et al vs. Chile* confirmed:

> *"the right of all individuals to request access to State-held information …[and] the right of the individual to receive such information and the positive obligation of the State to provide it, so that the individual may have access to such information or receive an answer that includes a justification when, for any reason permitted by the Convention, the State is allowed to restrict access to the information in a specific case* [*Claude Reyes et al vs. Chile*, paragraph 77 of judgment of 19 September 2006].

In conformity with this it is positive that the Montenegrin Law on Free Access to Information clearly states at Article 1 paragraph 3 that the right shall be guided by international human rights law. This provision is important as it should guide the court in their interpretation of the law (as has already happened in at least one Supreme Court ruling) and should assist drafters in their reworking of the law.

1.1. Provisions of the Law that Uphold the Right to Information

In line with Montenegro's obligations under international human rights law the LFATI contains a number of well-drafted provisions of principle that clearly establish the right to information. These include:

- The principle of publicity of government-held information (Article 1, paragraph 1 and Article 2.1);
- That principle that everyone (all legal and natural persons) may request information (Article 1, paragraph 2; Article 4.5);
- The principle of non-discrimination against those who exercise their right to information (Article 2.2);
- The right of access – barring application of legitimate exceptions – to all information held by public bodies (Article 1 paragraph 2, Article 4.1)
- A definition of public bodies that includes all bodies performing public functions or operating with public funds (Article 4.3).
- The principle of ensuring easy exercise of the right, summed up by the Council of Europe Recommendation 2002(2) at Principle V which states that *"Formalities for requests should be kept to a minimum."*. The Montenegrin law respects this in principle in Article 2.3 and 2.4;
- The principle that access to information should be prompt (Article 2.4) and the timeframes established by the law (8 days for an initial decision) is in line with comparative standards.

As we note in subsequent sections, however, some of these principles are not upheld by the detailed procedural provisions of the law. For example, although as we note at Section 4 below, there are in fact problems with the access provisions of the law as far as the right to copies is concerned.

1.2. Responsible Officials and the Duty to Assist

The LFATI contains in the definitions provision (Article 4) a reference to the "responsible person" for acting upon requests for information. The law also requires all public bodies to publish "the names of the persons authorized to act upon any request for the information" (Article 5). These provisions do not, however, provide a clear requirement that every public body appoint at least one person responsible for handling requests for information. The majority of access to information laws required that at least one person in each public body be nominated as the Information Officer responsible for receiving and following requests for information and for ensuring that information is delivered to the requestor within the timeframes established by law as well as ensuring compliance with other provisions of the law, such as proactive publication of material and keeping statistics on the number of requests and on the information delivered.

Such a person should always be different from the spokesperson of the entity as the function is quite different. In larger institutions, this should be a dedicated person, and in the largest central government bodies, more than one person should be appointed. In all cases, a deputy or substitute should also be nominated to ensure that when the Information Officer is out of the office for more than one day (meetings, travel, vacation, sick leave) there is a someone who is available to handle requests).

The public body should be obliged to publish the names, e-mails and office phone numbers of both the Information Office and the substitute on their website, in other public places, and in all materials it produces about the right of access to information.

We also note that the existence of an Information Officer does not imply any lessening of the ultimate responsibility held by the head of the body for compliance with the law. Nevertheless, the Information Officer should be empowered to take decisions on the release of information, especially routine information (See Section 8) , without the need to consult with senior officials. Indeed, some laws require that only decisions to refuse information should require internal discussion and a formal decision and decisions to release information should be more automatic.

Another function of the Information Officer is to provide assistance to requestors seeking information. We note that Article 17 permits public bodies to request clarifications from requestors as to the nature of their requests, but fails to require that they be assisted in formulating the requests so as to be sufficiently clear for the public authority to be able to act on them. We note that the Council of Europe Recommendation 2002(2) clearly states and Principle VI.5:

> *The public authority should help the applicant, as far as possible, to identify the requested official document, but the public authority is not under a duty to comply with the request if it is a document which cannot be identified.*

The LFATI contains the second part of this principle, but fails to include the first part. This should be rectified. If the requestor believes that the request is sufficiently clear, the public authority is under an obligation to accept this and to endeavour to process the request. The lack of clarity of the request should only be the grounds for a rejection after a demonstrable effort by the authority to help the requestor identify the information and a good faith effort to answer the request.

The powers of the Information Officer include taking a decision to release information without the absolute obligation to consult with the head of the body or other official. It is recommended, however, that they do not have the right to refuse information and that the decision to refuse information be taken by either the head of the institution (who in any case has legal responsibility for the decision), or by a nominated committee of senior officials.

Recommendations

- Introduce a clear provision requiring each public body to nominate an official responsible for the access to information process (the "Information Officer") and to publish his/her name on the website as well as office phone and e-mail address, and mailing address for sending requests.
- A deputy/substitute information officer should be nominated and his/her name and contact details also made available to the public.
- Introduce to the law a provision establishing a duty to assist requestors. The duty should include helping all requestors formulating requests, helping requestors identify the correct body for filing requests, and helping disabled and illiterate requestors set down requests in writing. Failure to provide such assistance should considered a breach of the LFATI and subject to a penalty imposed on the institution.

1.3. Requests for Information: Written and Oral

The law establishes provisions on requesting information that are broadly line with international and comparative standards. It is positive that the requestor does not have to pay a fee for accessing the information and it is implied (although not explicitly stated) that they do not need to provide reasons for asking for the information.

With respect to the information that the requestor must provide, it is positive that the requestor only has to provide a basic description of the information required as well as the optionally any additional information that may help identify the data they are looking for. It is also positive that the authority may not impose a form for requesting information.

On the other hand the law requires that the requestor provides basic data about him or herself, (name and address). We recommend that an e-mail address should be sufficient for requests submitted by e-mail.

The law permits requests in writing on paper or by e-mail, but unfortunately does not permit oral requests. We recommend oral requests when the requestor is asking for any information that should or may be available immediately (see section on proactive publication of information). For instance, a requestor should be able to walk into a government body and ask verbally for information such as an annual report without the necessity to fill in a request. Similarly, it should be possible to ask for the same information by telephone and have it mailed. Only in cases where the information is not immediately available or where the information would take time to compile in order to answer the request should the requestor be obliged to set down the enquiry on paper.

In particular the right to file oral requests should apply to all handicapped requestors for whom writing is a problem. Similarly those who are illiterate or with low levels of literacy should have the right to file oral requests. In these cases, the Information Officer or other official attending to the public should have the obligation to set the request down for them in writing.

Recommendations

- That the law be amended to make clear that an e-mail address is sufficient for answering requests.
- That oral requests be permitted when requesting information that should be available proactively or free of charge (see Section 8 on Proactive Publication / Routine Information)
- That law should establish oral requests for those who are handicapped or have low levels of literacy. The law should make clear that in such cases the Information Officer or other official should set the information down in writing for the requestor.

1.4. Forms of Access

One of the deficiencies of the drafting of the law which has already caused significant problems is the lack of clarity over the forms of accessing the information once the request has been granted. The law at Article 12.2 clearly allows the requestor to specify the form of access (meaning the format in which the information is contained) and Article 13 establishes the options for receiving the information (inspection, transcription, copies). Article 13 also establishes that in cases of partial access, only copies will be permitted as clearly inspection will not be an option, which is acceptable. However, Article 18 paragraph 5 opens the door to the government agency to make an resolution on access that limits access to inspection only.

These provisions have lead to problems in practice with some institutions asserting a right to offer inspection of documents only (which lead to some severe problems in practice for requestors seeking information that was clearly in the public interest when they were not allowed even to transcribe key data, nor to take photos or make voice notes during the inspection).

The Supreme Court decided on this matter in its ruling of 19 December 2006 (Supreme Court of the Republic of Montenegro, ref. 83/2006) which stated that:

> The provision of Article 13 of the Law on Free Access to Information stipulates the manner for exercising the right to access information where one of the envisaged possibilities is to have direct inspection of public records, the original or the copy of the information, at the premises of the given authority. This, however, does not imply the arbitrariness of the authority to stipulate the manner of access at own discretion. The authority has the primary obligation to consider the possibility for the exercise of this right in the manner stated in the request."

The Supreme Court ruling is consistent with international law, which provides a right to "seek, receive and impart" information. Reception and imparting would clearly be hindered by not having a copy of the information. Such an interpretation echoes comparative standards where the majority of laws permit requestors to obtain a copy of the documents that contain the requested information. Indeed, the problem that arose in Montenegro is rather perverse in that the usual problem is with inspection of originals because of cases in which such inspection could damage historic documents.

If a public body lacks the facilities for making photocopies of all the information requested, it should be under an obligation to make arrangements with another public body to produce such copies. The need for such external support in producing copies may never be a reason for either denial of the request or for extension of the time-period in which access must be given.

It is positive that the law establishes (Article 7) that those with disabilities should be provided with information in the form that they can use it and that the public body may not require them to pay fee for this conversion (Article 12, paragraph 2).

Recommendations

- That the law be amended to make clear that there is a right of copies to documents
- That the law make clear that inspection is almost always an option in addition to the right to receive copies but that they are not mutually exclusive (ie: a requestor may ask to see originals in situ and then request copies).
- That the law make clear the obligation on public bodies to find a solution to the copying problem.
- Amend Article 18 paragraph 5 to make clear that access by inspection or transcription will be only when requested by the applicant. The law should retain the unlimited timeframe for exercising such access.

1.5. Time Frames

The 8 calendar-day timeframe for responding to requests established by Article 16 is in line with international standards on access to information. In practice, if the last day of a deadline falls on a non-working day, the day for provision of the response would be the first subsequent working day. However, when calculating the deadlines, non-working days are included in the count.

It is also positive that there is a 48-hour time limit for emergency information (as per the rules noted above, if a request were filed on a Friday afternoon, the response would be due on the Monday).

We note that the timeframe comes into force from the day the request was received by the authority. In the case of hand delivered requests, this will be clear as there should be some receipt given for the request with a reference number. In the case of requests submitted by post (registered or otherwise) and by e-mail, we recommend that the authority be obliged to issue a receipt note (a letter or e-mail containing a registration number) in order to confirm the receipt date and to facilitate subsequent tracking of the request.

Article 18 paragraph 4 provides that once a decision on access has been reached, access shall be provided within three calendar days in the case of copies being provided (Article 18, paragraph 5 establishes an unlimited timeframe for inspection). The means that maximum time-frame for access shall be 11 calendar days from the filing of the request.

We note that Article 15 requires that requests be treated "in a summary procedure" and note that while this is a good principle for putting in the opening provisions of the law, its location in Article 15 is perhaps redundant.

The extension for voluminous requests of up to 15 calendar days is reasonable and fits with comparative standards on timeframes. The law should,however,contain an obligation that if such an extension is to be applied,the requestor should be notified within the initial 8 days established by law for responses, and they must be informed about how long the extension will be and must be provided with a clear written justification as to why the extension is being applied.

Clarifications: Another timeframe is established in the Article 17 provision on "eliminating deficiencies" from requests (we recommend "clarifications" as a better terminology in English). This provision says that if the request is incomplete or unclear, the public body can require the

requestor to clarify within 8 calendar days. The timeframe for answering such a clarified request appears to be the same as for initially submitted requests, so 8 calendar days (although Article 17 paragraph 3 is not completely clear, at least in the English translation).

The law fails, however, to stipulate the timeframe for the body to contact the requestor. We presume that it might be the 8 days initially given for response but we believe this is too long and strongly recommend that this should be a short time-frame, for example **3 calendar days**. The requestor should then be at liberty to submit a reformulated request at the time of her or her own choosing, and once the request is received, the public body has 8 days for answering.

Timeframes and Basis for Appeals: It is positive that when an appeal is submitted, the first level institution (against which the appeal is made), has just 3 days to prepare their case (Article 21) and to transfer the appeal to the responsible second-level institution together will all related documents. The second level then in turn has to make a decision within 15 days of the submission of the complaint (Article 22). These are suitable deadlines for the important matter of an appeal against a refusal or failure to release information.

We note however that the law at Article 20 establishes that an appeal may be made against "any document … deciding upon any request for information". The law should be amended to make clear that administrative silence may also be appealed and that if the requestor has not heard anything from the entity within 8 days of submission of the requests (or an additional 15 days if an extension was notified by the agency) then there an automatic right of appeal. The law should also establish whether administrative silence is positive or negative. We note that in some countries the access to information law establishes administrative silence as positive (something common in Administrative Law), which facilitates an immediate appeal to the Information Commissioner which in turn can order the immediate release of the document. Other FOI laws qualify administrative silence as negative (sometimes going against the norm of Administrative Law) in order to provide legal grounds for an immediate appeal against the failure to respond to the request.

Recommendations

- We recommend that the law be amended to require that in the case of extensions being applied,the public body must notify the requestor within 8 calendar days and must inform the requestor of the reasons for the extension and the length of it (not all extensions will be for 15 days:each extension needs to be justified and some may warrant only a few extra days).
- There are some additional timeframes that are common in other access to information laws that are missing from the LFATI and that are necessary for fully effective implementation of the law. These include:
  - We recommend introduction of a short timeframe for initial review of the request: if the authority determines that the holder of the information requested is another public body, it should be obliged to transfer the request to that body within **3 calendar days** and should inform the requestor that this has been done.
  - If there is no response to a request within **8 calendar days** from the date when it was filed (or an additional 15 days in the case of an extension having been notified), then the requestor may appeal this immediately.
  - The law should establish if administrative silence is positive or negative.

1.6. Fees

It is positive that the law prohibits a fee for filing requests (Article 11, paragraph 3) and that only the costs of reproducing the information (copying, transcribing) may be charged (Article 19 paragraph 2).

However we understand that no regulation has been introduced to establish the costs to be charged in spite of the fact that Article 19 refers specifically to a separate regulation. This is causing problems in practice because different institutions are establishing different costs, including those that are not real costs: for example, there are instances when they charge copying of one page € 0.50, although real costs would be maximum € 0.01 (the street cost of copying is around 10 eurocentimes; given that street photocopiers are a commercial enterprise, government costs should fall below this). .

It is an unfortunate weakness of the drafting of the law that it does not make clear who is responsible to adopt such a regulation, nor that it should be unified for all institutions. We strongly recommend that such a harmonized resolution on minimum costs urgently be introduced, either by the Ministry of Finance or by the Ministry of Culture and Media, the institution is responsible for LFATI, as appropriate.

In addition we recommend that the information that is subject to proactive disclosures under Article 5 (lists of types of information held, registers, procedures for access) as well as the new provisions on Proactive Publication of information (See Section 8) should introduce a class of information that is not subject to charges. This is to ensure that the basic information that has already been created with the tax-payers money (for example, annual report and accounts of government bodies, information about their core functions, etc) is available to all members of the public without the need for any extra payments (which almost amounts to a double taxation).

We also recommend that consideration be given to the introduction of a fee waiver for

i. small numbers of copies where the monies collected by the state are less than the costs of processing the payment. In some countries the first, 20 or 50 pages are free of charge by law, and in practice often documents of up to 200 pages are handed out free of charge.
ii. for indigent requestors (there needs to be an exploration of how this would be demonstrated, such as if a person is already receiving welfare payments from the state). Criteria might include, for example, those whose income (salary or other income such as pension) has been established as being lower than the official extreme poverty line of €117 per person per month, the unemployed, and those receiving social welfare.

The Information Commissioner should review the fees charged by each body for photocopying and materials, and make recommendations and in some cases recommend sanctions if the charges are being used in any way as an obstacle to the right to information.

Recommendations

- Introduce a regulation that sets maximum charges for photocopying and costs of other materials, making clear that on-site inspection and electronic delivery of information should always be free of charge;
- Introduce a fee waiver for small numbers of copies and for indigent requestors;
- Amend the law to ensure that all information that should be published proactively is available free of charge;
- Empower the Information Commissioner to inspect costs charged and to make recommendations as well as to sanction bodies found to be violating the costs provisions.

1.7. Exemptions: Information that may not be refused

A separate analysis examines in detail the exemptions provisions of the LFATI and their relation to other legislation. At this point we note that it is positive that the law contains harm and public interest tests.

We also note that it is particularly positive that Article 10 establishes that certain information may not under any circumstances be exempted from release to the public. There is a focus here on the classes of information that could expose abuse of power or corruption, including evidence of "disrespect to substantive regulations; unauthorized use of public resources; misuse of powers; unscrupulous performance of public duties; the existence of reasonable suspicions a criminal offence was committed; or the existence of the grounds for attacking a court judgment". Such information must be released under all circumstances, "regardless of the seriousness of damages caused to the interests referred to in paragraph 1 of Article 9 of this Law [on exemptions and protected interests] "

Whilst it may take some time for this provision to show its full value, we believe that it is a key element of the law and over time will underpin the value of the right to information in fighting corruption in Montenegro.

There are however other classes of information that could usefully be mentioned in Article 10 as being exempt from any restrictions on disclosure. Typically, these provisions refer to information that would expose violations of human rights (past, current or future violations), threats to public health and safety, and damage to the environment.

1.8. Proactive Release of Information

The Montenegrin law contains almost no requirements on what is known as proactive or *ex officio* publication of information, information that must be released without the need for a request. Under the LFATI, the only information that must be made public, as established by Article 5 of the law, is an obligation to compose and publish:

- a list of the types of the information filed with the body (including also public registers and records)
- data on the procedure for access to the information
- names of the persons authorized to act upon any request for access to the information
- other data of importance for exercising the right of access to the information (Guide for Access to Information).

Although this basic requirement is positive, it is out of step with comparative standards: most modern access to information laws contain a more extensive list of information that should be made available proactively.

In the pre-Internet age, the requirements in access to information usually required paper publication of core information related to the functioning of the public body. With most European public bodies now having extensive websites the requirements for proactive provision of information have expanded and in a number of countries new legislative provisions, known as e-FOIA laws (electronic freedom of information) have been adopted. At a minimum, such provisions require publication of large volumes of "routine" information that relates to the core functions of each obliged body.

Such comparative developments lead to the Council of Europe Recommendation 2002(2) including a number of relevant principles, including that

- Member States should take the necessary measures to "*inform the public about its rights of access to official documents and how that right may be exercised*" (Principle X on "Complementary measures" at 1.i)
- Member States should also "*as far as possible, make available information on the matters or activities for which they are responsible, for example by drawing up lists or registers of the documents they hold*" (Principle X, 2.iii).

In addition, a specific provision, Principle X, dedicated to "Information made public at the initiative of the public authorities", states that

> *A public authority should, at its own initiative and where appropriate, take the necessary measures to make public information which it holds when the provision of such information is in the interest of promoting the transparency of public administration and efficiency within administrations or will encourage informed participation by the public in matters of public interest.*

Typically, there are a number of categories of information that should be made available.

(i) Information needed for exercise of the right of access to information: such information would include indexes or register of information held. It would also include the name and contact information of the Information Officer and details on mechanisms for requesting information. This requirement is already included in the LFATI.

(ii) Financial, Structural and Administrative Information: this includes information on the budget and structure of the institution, which should include:

- **Organizational structure:** The organizational structure of the public body indicating all its organizational units, including departments and agencies under direction of the institution, with the tasks of the individual organizational units. This information should include the name, rank and contact information (phone and fax number, e-mail address) of the managers of the public body and the managers of the individual organizational units, agencies, etc.
- **Budget Reports**: the public body's annual report and accounts as well as projected budget for the current year, and all reports on actual income and on the expenditure of the budget for current year to date, including budgetary and extra-budgetary incomes and expenditures.
- **Employee Financial Information**: summary information concerning the number of employees and their remuneration (by position and/or by name according to domestic law, but preferably by name), as well as a summary of the type and amount of benefits granted to employees. For managers and senior officials, information on wages, fringe benefits, regular benefits and expenses reimbursement.

(iii) Administrative, Decision-Making, Information needed for Participation

Traditionally information that relates to the core functioning of a public body has been available. Information has often been available after decisions have been taken. In modern democracies it is expected that information will also be made available in advance of decisions being taken in order to permit public comment and contributions. Information on policies under consideration, draft regulations, planned budget expenditures, should all be made available.

(iv) Information needed for ensuring probity (anti-corruption information)

Another class of information that it is increasingly common for laws require to be made public is information needed to ensure financial probity. It is widely accepted that transparency of financial information reduces the potential space for corruption. Such information would typically include:

- ***Assets Declaration***: assets declaration of, at least, the head and senior officials of the body. All appointed and public officials with responsibility in areas where there is a high risk of corruption should be required to submit assets declarations.
- ***Declarations of Interests***: the declarations of external interests of senior public officials, particularly where there may be a conflict of interest such as their membership on the board of a company that receives public procurement contracts.
- ***Gifts declarations***: declarations of gifts received by senior public officials, with information on the source and value of the gift (in some countries gifts over a certain value must be handed over to the public body rather than retained by the minister or other official).

(v) Information on the Public Procurement Process

The public body should publish key information related to the public procurement process. This information should include:

- **List of contracts:** the public body should publish a full **l**ist of all contracts concluded with external suppliers of goods, services, etc., including the name of the contractors and the value of the contract and summary of nature of goods/services to be provided.
- **List of concessions/licenses:** List of all concessions/licences granted by the Public Institution, together with the value, and summary of the nature and duration of the concession/licence.
- **Details on public procurement / tender processes** including **details of upcoming tenders,** public bidding guidelines or terms, financial and technical specifications, selection criteria and the weighting given to these criteria. Details should be made available on all those who competed, with fuller details on the winner of the tender, as well as the **contract** itself being made available. Whilst there will be some commercial secrets exemptions applied here, comparative jurisprudence makes clear that the majority of contract information must be made public.
- **Evaluation of compliance with contract conditions**, as well as any sanctions imposed by the public body for non-compliance with the contract or for failure to meet deadlines.

Recommendations

- The LFATI should be amended to include provisions requiring proactive release of information.
- The LFATI should be amended to require that all proactive information should be provided free of charge.

1.9. Environmental Information

Montenegro's constitution at Article 1 establishes, *inter alia*, that Montenegro is a "ecological state". The importance of access to environmental information is such that there is an international treaty dedicated to this, the UN/ECE Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters, known as the Aarhus Convention. Montenegro has not yet signed the Aarhus Convention.

The European Union's Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information, incorporate the principles of the Aarhus Convention. We note that the European Union signed the Aarhus Convention on 25 June 1998 as a result of which, provisions of Community law must be consistent with that Convention, so for future EU membership, Montenegro will need to harmonize its law with these provisions.

In the meantime, Montenegro can prepare for the ratification of Aarhus and compliance with EU standards by ensuring that its own legislation contains requirements on disclosure of environmental information (and on concomitant public participation). Such provisions should refer to private bodies as well to the extent required by Aarhus. The relevant Aarhus provisions state that :

> *3. "Environmental information" means any information in written, visual, aural, electronic or any other material form on:*
> *(a) The state of elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites, biological diversity and its components, including genetically modified organisms, and the interaction among these elements;*
> *(b) Factors, such as substances, energy, noise and radiation, and activities or measures, including administrative measures, environmental agreements, policies, legislation, plans and programmes, affecting or likely to affect the elements of the environment within the scope of subparagraph (a) above, and cost-benefit and other economic analyses and assumptions used in environmental decision-making;*
> *(c) The state of human health and safety, conditions of human life, cultural sites and built structures, inasmuch as they are or may be affected by the state of the elements of the environment or, through these elements, by the factors, activities or measures referred to in subparagraph (b) above.*

Recommendations

- Montenegro's law should ensure full access to environmental information in line with the Aarhus Convention and European law. This is particularly appropriate for a constitutionally ecologic state.

1.10. Relation with the Archives Law

There is a need to clarify whether or not the Free Access to Information Law will applies to all information held in the historical archives in Montenegro. We strongly recommend that the right to information does apply to all information held by all parts of government, with necessary exemptions for access to historic documents that are in a delicate physical condition. The right of access as established by international law applies not only to current documents but to all documents held by public bodies, irrespective of their date of creation.

1.11. Whistleblower Protection

The LFATI contains a form of "whistleblower" provision in Article 25 of the law which establishes that any official who, acting in good faith in accordance with his/her duties, releases information that reveals misconduct or abuse of power by any other official, may not be penalized for such disclosure, provided that they inform the head of the authority or the relevant investigative authority.

The provision says that any employee who discloses such information may not be held accountable. It is presumed that the information is not released following an information request, although this should be clarified.

However, the location of this provision in the access to information law seems to imply that it might also refer to officials who release information to the public following an information request. In that case the official is only exempt if they also inform their superior or an investigative agency. This could be complex in practice. For example, imagine a case in which an official is asked to release information including budget expenditure details, copies of public works contracts and other information held by a particular public body. Imagine then that when this information is examined by the requestor (an investigative journalist or NGO for example), it shows that there has been some wrongdoing. But the public official who passed on the information, was not aware of this as she/he had not compiled the different documents and analysed them, but merely provided a collection of documents in response to the request. In that case, the official would not have informed his or her boss or other body, and this provision would not apply to them.

Recommendations

- It is positive that the Montenegrin law contains a whistleblower protection. It could be further clarified to ensure that it provides full protection to public officials who release information under the law.
- In parallel, a full whistleblower law that also protects those working in private companies who leak information of public interest, such as information revealing abuse or wrongdoing, should be adopted in Montenegro. The whistleblower law should include mechanisms for internal disclosure of information and for bodies to which whistleblowers can turn for support and protection.

1.12. Sanctions

The law establishes a number of penal provisions in the form of fines that may be imposed for violations of the law. The public agency and the responsible person may be fined.

The violations identified include failing publish the Guide for Access to Information that each body is obliged to produce (Article5); failing to enable inspection of public registers and records (Article6); failing to provide information in the form required by disabled persons (Article 7); and failing to provide access to the applicant (Article 8, which says that access must be provided barring legitimate exceptions established by the law).

There are also fines for violations of Article 9 (application exemptions) and Article 10 (requirement that all information exposing wrongdoing be published), as well as of Article 25 (the provision that says that no one may be penalized for exposing misconduct by another official).

What is not clear is who would initiate the process for some of these sanctions. For example, a number of bodies have failed to publish their Guides for Access to Information but so far there has been no sanction. And whilst there has been litigation to challenge failures to respond to information requests or misapplication of exemptions, this has tended to result in orders to release the information or review the administrative decision rather than a fine on the public body.

We also note that there is no distinction between lesser and more serious offences. For example, failing to publish the Guide for Access to Information is perhaps a lesser offence than repeated obstruction of requests or taking action against an official who has exposed corruption. Other offences that other access to information laws establish and that are particularly grave, such as willful destruction of documents, are not covered by this law and should be introduced.

Our main recommendation is that it should be the Information Commission, whose establishment is proposed in Section 14 below that should recommend the imposition of these sanctions. This Commission can then take appropriate action. For example, small government bodies may not have published the Guide for Access to Information because they have limited human resources and are not experts in the theme. In this case, it would be better if they were provided with assistance from the Information Commission rather than being fined.

We note that the object of the lighter sanctions should be to encourage the release of information and not to create any fear amongst public officials that they will be penalized if they release information. As such, they should be imposed with care and particularly for repeated violations of the law.

Recommendations

- Revise sanctions to make sure all possible offences that violate right to information are covered and that there is a range of sanctions depending on the gravity of the offence;
- More serious offences such as willful destruction of documents should be dealt with by this law and should also be established as criminal offences.
- Empower the future Information Commissioner to act *ex officio* on breaches of the law and to recommend sanctions.

1.13. Personal Data Protection.

The law makes references to protection of personal data insofar as this is one of the exceptions to the right to information. Specifically Article 9.3 provides that information should not be released if it would cause significant harm to:

> *privacy and other personal rights of individuals, except for the purposes of court or administrative procedures, through disclosing the information:*
>
> *a. concerning private lives of parties and witnesses in the procedures, as well as of victims and parties injured by criminal offences, and through disclosing the information of adjudicated persons;*
> *b. contained in personal and medical files of individuals, findings obtained from psychiatric and psychology examinations and personal disposition tests;*
> *c. relating to the establishment of parental rights, adoption of children and alike;*
> *d. regarding individual employment, income, pension, relief and other social welfare benefits;*
> *e. giving phone numbers, temporary or permanent residences of individuals and their families, if such individuals require a relevant authority to keep the information secret because they reasonably believe their and their families' safety is at risk;*

Whilst it is positive that the LFATI recognizes the right to privacy and elaborates on what this right means, such a provision does not substitute for a full data protection law: Montenegro needs a full data protection law that meets European standards on the right to data protection. This will become an absolute requirement in any future candidacy for EU membership.

The main elements of such a law include that all personal data held by any public or private body be subject to rules about how it is processed, stored, used, shared and transferred internationally. Individual members of the public should have a right to know what data is held about them and to receive a copy of that data. They should also have a right to challenge the accuracy of the data, and to have changes made or their comments appended to the data. Such a right clearly entails additional legal mechanisms that cannot be contained in an access to information law.

In addition, the fact that a data protection law obliges private bodies as well as public bodies clearly requires that an additional piece of legislation is adopted.

Data protection law is a complex body of law that is under constant evolution at the European and global level. The European Convention on Human Rights and Fundamental Freedoms recognizes the right at Article 8 on Right to respect for private and family life:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Numerous cases of the European Court of Human Rights have interpreted the scope of this right.

Within the EU, the necessities of the internal market and the trans-frontier nature of information flows have resulted in data protection law being harmonized across all EU member states in line with EU directives (the first is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and jurisprudence of the European Court of Justice (for more information see: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm).

There is an EU requirement that a each country has a national Data Protection Commissioner to oversee data protection law and hear complains. In many countries such oversight is combined with oversight of the right to information in a single Information Commissioner operating with separate departments specialised in each issue. We recommend this as an appropriate solution for Montenegro. A good model to study would be the Slovenian Information Commissioner which, since January 2006, has combined the access to information and the data protection functions.

Recommendations

- Montenegro should introduce a personal data protection law.
- The government should work with civil society to develop this law.
- It would be appropriate if the Information Commissioner were also responsible for oversight of the data protection law.

1.14. Information Commission or Information Commissioner

An increasing number of countries worldwide have an Information Commission or Commissioner to oversee the access to information law. Examples in Europe include Commissioners in the UK, Ireland, Germany, and Hungary and Commissioners in France and Portugal. Globally too, Canada and Australia have commissioners at national and regional levels and Mexico has Commissions at Federal and state level. In the former Yugoslavia, Serbia and Slovenia have Commissioners, Macedonia has a Commission and Bosnia has the Deputy Ombudsperson responsible for this issue. The great advantage of these institutions is that help the administration with the implementation of the law and provide a fast and low-cost forum for deciding on disputes over information requests. We note that countries that have an Information Commissioner generally have a much more successful implementation of the Access to Information law. This is a more effective mechanism than the Ombudsman because the Ombudsman has many other duties and cannot dedicate sufficient resources to the right to information.

It is strongly recommended that Montenegro follows this trend and institute a body that will oversee the implementation of the law. There is little difference between a Commissioner and Commission in terms of their powers. A Commission has the advantage of having more members who can specialize in different areas (access to information, data protection, information management, e-governance) and support each other in decision-making. It also creates the possibility of electing a rotating membership that is less susceptible to political pressures.

Whether there is one Commission or more than one Commissioner, the responsible persons should be selected by an open process in which there are nominations from different sectors of society including civil society and open hearings before the person is appointed. The candidates for Commissioner(s) should be persons who have a track record in related professions and not have a political background. For example, in the UK the Commissioner is a lawyer with experience in consumer rights, his two deputies have worked in local government and trades unions respectively. The Hungarian Commissioner was a lawyer and political scientist who worked to promote the right to information as far back as the 1980s, the Irish Commissioner was a political correspondent; the Slovenian Commissioner has a law and communications background.

The role of a Commissioner is not to defend the requestors nor the government but to defend the right to information. This means defending the principle of open government and also protecting the legitimate interests such as national security, commercial secrets and protection of personal data. The Commissioner's job will be to make sure that the right to information functions smoothly in practice and that any limitations are appropriately applied and subject to the public interest test. The benefit of a Commissioner is that it builds up experience over time and can provide a specialized understanding of the issues whether the task it to recommend an information management system or adjudicate over a disputed information request.

The mandate of the Commissioner should be to promote and protect the right to information, rule on appeals against refusals to provide information and promote the right to privacy and protection of data held by public and private bodies. The Commissioner should have the following powers and duties which are drawn from a comparative analysis of Commissioner's offices worldwide:

- Operational independence: designs its own internal regulation; defines its budget and staff structures;
- Reports annually to parliament on the implementation of the law, including with statistics gathered from every public body and other research that it carries out;
- Promotes public awareness of the right to information through creation and dissemination of guides on how to file requests, publicity materials and by engaging in public debate about the right to information;
- Trains and assists public officials in how to implement the law and is ready to respond with guidance on specific requests;
- Produces guidance on particular aspects of the law and on how to apply exemptions (see for example the excellent guides produced by the UK Commissioner's Office http://www.ico.gov.uk/tools_and_resources/document_library/freedom_of_information.aspx
- Helps the administration with the design of systems for filing requests electronically (possibly through a unified electronic requesting system as in Mexico)
- Monitors compliance by public authorities with provisions of the law that require proactive publication of information and development of citizen guides;
- Promotes the appropriate classification of information (as will be regulated by the future state secrets law in Montenegro, as well as under laws regulating commercials secrets)

including through having the power to review classified documents both ex officio and when there is a disputed information request;
- Receives and reviews complaints from requestors about refusals, partial answers, incomplete answers, administrative silence (failure to answer requests at all) and other alleged breaches of the right to information. The Commissioner becomes the first instance body for hearing and ruling on complaints in the way that in Montenegro is currently handled by the courts. The Commissioner decides on a case by confirming or overturning administrative decisions, and where appropriate by ordering release of the information;
- Recommends sanctions against public bodies that have violated the law;
- Participates in court processes related to the right to information and data protection either as an expert witness or by submitting *amicus curiae* briefs as appropriate;
- Proposes to parliament legislative reforms necessary for ensuring better respect for the right to information and right to personal data protection;
- Represents Montenegro in international forums where issues of the right to information and data protection are being debated;
- Liaises with all members of society including the administration and civil society organizations on how to ensure the right to information is fully respected in Montenegro.

For reference the following websites provide further insight into the functioning of selected Commissions and Commissioners (all have sites in English and/or southern Slavic language):

United Kingdom Information Commissioner's Office	http://www.ico.gov.uk/
Scotland Information Commissioner	http://www.itspublicknowledge.info/
Slovenian Information Commissioner	http://www.ip-rs.si/index.php?id=126
Ireland's Information Commissioner	http://www.oic.gov.ie/en/
Berlin Information Commissioner	http://www.datenschutz-berlin.de/ueber/aktuelle/inheng.htm
Serbian Information Commissioner	www.poverenik.org.yu
French CADA	www.cada.fr
Mexican Information Commission	http://www.ifai.org.mx/
Macedonian Information Commission	http://www.sinf.gov.mk/

Recommendations

- Montenegro should introduce an amendment to its Law on Free Access to Information that will result in the establishment of an Information Commission or Information Commissioner. This should be treated as an urgent priority for ensuring full implementation of the LFATI.
- The government should work with civil society to develop this law and should take into consideration the experience of other European countries that have such a law, including the countries in the South East Europe region.
- It would be appropriate if the Information Commissioner were also responsible for oversight of the data protection law.

PART II

PROVISIONS ON SECRECY AND EXEMPTIONS IN LAW ON FREE ACCESS TO INFORMATION AND RELATED LEGISLATION

Introduction

The purpose of this analysis and recommendations is to propose ways in which Montenegro's Law on Free Access to Information (LFATI) and related legislation should be interpreted and amended in order to ensure full compliance with the right of access to information.

Montenegro has a full access to information law adopted in November 2005 which contains a list of exemptions to the public release of information. Montenegro since its independence has not adopted a new law on state secrets nor has it harmonised laws on commercial secrets with modern European standards.

In this analysis we first present the standards that Montenegro is obliged to uphold when establishing any secrecy legislation, we then analyse the exemptions provisions of the existing LFATI in the context of these standards, and finally consider the main elements of other legislation that should also be introduced/amended, notably the state secrets law.

In conducting this analysis, we have been guided by established international standards, including the provisions of the ICCPR and ECHR, and the Recommendation 2002(2) of the Council of Europe on Access to Official Documents. We have also drawn on comparative law and jurisprudence, particularly that from the member countries of the European Union.

2.1. Exemptions to the right of access to information permitted by international law

The right to information is a fundamental but not an absolute right. This is clearly established by the provisions of international law that provide for a right of access to information. For example, Article 10 of the European Convention on Human Rights and Fundamental Freedoms provides the right to "*to receive and impart information and ideas without interference by public authority and regardless of frontiers*."

The permissible restrictions are set out in Article 10(2) which sets forth that "*[t]he exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*."

In practice the European states that have adopted freedom of information laws have defined a slightly different list of exemptions which function more logically in practice when it comes to the exercise of the right to information. This list is encapsulated in the Council of Europe Recommendation 2002(2), adopted by the Committee of Ministers in 2002 and currently being converted into a binding treaty which all Member States of the Council of Europe (including Montenegro in due course) will be expected to sign and ratify. This treaty will be important in that it will establish a limited regime for exemptions to the right of access to information and will not permit any other legislation that establishes a broader secrecy regime. In other words, Council of Europe member states will have to harmonize their legislation with this set of exemptions.

Council of Europe Recommendation 2002(2) at Principle IV sets out the permissible exemptions:

IV. Possible limitations to access to official documents*

1. Member states may limit the right of access to official documents. Limitations should be set down precisely in law, be necessary in a democratic society and be proportionate to the aim of protecting:

i. national security, defence and international relations;
ii. public safety;
iii. the prevention, investigation and prosecution of criminal activities;
iv. privacy and other legitimate private interests;
v. commercial and other economic interests, be they private or public;
vi. the equality of parties concerning court proceedings;
vii. [nature];
viii. inspection, control and supervision by public authorities;
ix. the economic, monetary and exchange rate policies of the state;
x. the confidentiality of deliberations within or between public authorities during the internal preparation of a matter.

2. Access to a document may be refused if the disclosure of the information contained in the official document would or would be likely to harm any of the interests mentioned in paragraph 1, unless there is an overriding public interest in disclosure.

3. Member states should consider setting time limits beyond which the limitations mentioned in paragraph 1 would no longer apply.

** NB: as noted elsewhere in this document, this list is currently under revision and Montenegro's legislators would be advised to verify the actual text of the future treaty which is currently being drafted by the Council of Europe.*

Although likely to be subject to some modification during the treaty drafting process, the essence of these exemptions is likely to remain. In Section N** below we analyse the current Montenegrin Law against these exemptions.

The countries of the Council of Europe region are all in the process of reforming their secrecy laws to ensure better harmonization with the right of access to information; this is not a challenge for Montenegro alone. As a recent report from the OSCE Rapporteur on Freedom of the Media notes:

> *Modern FOI principles constitute a Copernican revolution for the development of the free press. By passing them either as Constitutional amendments or basic laws, the states give up their absolute right to withhold information, and introduce the primacy of their citizens' right to know about the government, making it an exception defined in law when the government still has the right to classify information.*[1]

[1] "*Access to information by the media in the OSCE region: trends and recommendations*" Vienna, 30 April 2007, at page 1

The reality is, however, as the OSCE Rapportuer concludes, that this "Copernican revolution" – this paradigm shift – is not yet complete: "*Unfortunately, many countries … have not yet adjusted their rules of classification to the FOI principles, that is, they disregard the primacy of the public's right to know*."[2]

In order to overcome this situation, the OSCE makes a series of recommendations that are directly relevant for Montenegro given that it is in the process of reforming its legislation at this point in time. First are the principles that should be included in any access to information law:

An Access to Information Regime Should Ensure that …

- Some information of a sensitive nature may be subject to withholding for a limited, specified time for the period it is sensitive.
- The exemptions should be limited in scope.
- The official who wishes to withhold the information must identify the harm that would occur for each case of withholding.
- The public interest in disclosure should be considered in each case.
- In cases where information may be deemed sensitive by any other law, the FOI law must have precedence.

This principle is followed be a series of recommendations for any state secrets and related legislation, which Montenegro should incorporate into it's future laws:

OSCE Recommendations on classification rules

- The definition of state secrets should be limited only to data that directly relate to the national security of the state and where their unauthorized release would have identifiable and serious consequences. Information designated as "Official" or "work secrets" should not be considered for classification as state secrets. Limits on their disclosure should be found in the access to information law.
- Information relating to violations of the law or human rights, maladministration or administrative errors, threats to public health or the environment, the health of senior elected officials, statistical, social-economic or cultural information, basic scientific information, or that which is merely embarrassing to individuals or organisations should not be classified as a state or official secret.
- Information should only be classified as a state secret for a limited period of time where the release of the information would cause a serious harm to the interests of the nation.
- Information that is classified should be regularly reviewed and have a date after which it will be declassified and released. It should be presumed that no information should be classified for more than 15 years unless compelling reasons can be show for withholding it.
- Governments should institute a review of all secret information over 15 years old and automatically declassify and release it. All information that was designated as secret by a previous non-democratic government should be declassified and presumptively released

[2] "*Access to information by the media in the OSCE region: trends and recommendations"* Vienna, 30 April 2007, see page 4

unless it is shown that its release would endanger the national security or be an unwarranted invasion of privacy.

- An independent body that is not part of the intelligence, military or security services should have oversight over classified information and ensure that the system is operating properly, receive complaints about improperly classified information and review and order the declassification of information.

The OSCE report is important as it is a synthesis of the current standards in Europe and directly applicable to Montenegro.

Another source of secrecy regulation in Europe are the requirements for classification of documents shared between NATO states. Although only directly relevant for NATO members and members of the Partnership for Peace, these standards are nevertheless useful to take into consideration when drafting the future secrecy laws in Montenegro. NATO standards establish four levels of classification for information Top Secret, Secret, Confidential and Restricted. There is actually a 5th category, which is "Unclassified". As NATO notes in its 2002 document on Security of Information:

> *"the classification assigned determines the physical security given to the information in storage and transmission, its circulation, destruction and the personnel security clearance required for access. Therefore both over-classification and under-classification should be avoided in the interests of effective security as well as efficiency."*[3]

NATO recommends that all classification be reviewed at least every five years unless the originally classification allocated to the document was predetermined to be automatically downgraded after two years[4]. It is important to note that such time frames in a security-sensitive organization like NATO contrast with the tendency for longer classification periods in many countries around the world. This indicates that where there is a need to balance real security with the efficiency of a security operation then in most cases information will only have any potential to cause real harm for a very limited period of time.

As noted above, however, the OSCE recommends that an access to information law should always take precedence over a state secrets law, and hence the time period for classification is in some ways less important than the fact that when a request for information is received, the relevant official reviews the information to determine whether it would indeed cause harm to a protected interest by being released.

Finally another source of standards on the classification of information on grounds of national security are the Johannesburg Principles[5]. Adopted in 1996 by a experts in international human rights law, the Principles were subsequently endorsed by Mr. Abid Hussain, the UN Special Rapporteur on Freedom of Opinion and Expression, in his reports to the 1996, 1998,1999 and

---

[3] NATO, Enclosure "E" to C-M(2002)49 at paragraph 4.
[4] NATO, Enclosure "E" to C-M(2002)49 at paragraph 6.
[5] The Johannesburg Principles were adopted on 1 October 1995 following consultations with and a meeting of 35 experts in international law, national security and human rights convened by the organization Article 19 (London). See http://www.article19.org/pdfs/standards/joburgprinciples.pdf.

2001 sessions of the United Nations Commission on Human Rights, and referred to by the Commission in their annual resolutions on freedom of expression every year since 1996.

The basis for the Johannesburg Principles is the same as that found in other areas of international law: namely that any "no restrictions on freedom of expression and [access to] information on the ground of national security may be imposed unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest. The burden of demonstrating the validity of the restriction rests with the government."

Johannesburg Principles On National Security[6]

Section III. Restrictions On Freedom Of Information

Principle 11: General Rule on Access to Information
Everyone has the right to obtain information from public authorities, including information relating to national security. No restriction on this right may be imposed on the ground of national security unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest.

Principle 12: Narrow Designation of Security Exemption
A state may not categorically deny access to all information related to national security, but must designate in law only those specific and narrow categories of information that it is necessary to withhold in order to protect a legitimate national security interest.

Principle 13: Public Interest in Disclosure
In all laws and decisions concerning the right to obtain information, the public interest in knowing the information shall be a primary consideration.

Principle 14: Right to Independent Review of Denial of Information
The state is obliged to adopt appropriate measures to give effect to the right to obtain information. These measures shall require the authorities, if they deny a request for information, to specify their reasons for doing so in writing and as soon as reasonably possible; and shall provide for a right of review of the merits and the validity of the denial by an independent authority, including some form of judicial review of the legality of the denial. The reviewing authority must have the right to examine the information withheld.

Principle 15: General Rule on Disclosure of Secret Information
No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

Principle 16: Information Obtained Through Public Service
No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.

Principle 17: Information in the Public Domain
Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know.

Principle 18: Protection of Journalists' Sources
Protection of national security may not be used as a reason to compel a journalist to reveal a confidential source.

Principle 19: Access to Restricted Areas
Any restriction on the free flow of information may not be of such a nature as to thwart the purposes of human rights and humanitarian law. In particular, governments may not prevent journalists or representatives of intergovernmental or nongovernmental organizations with a mandate to monitor adherence to human rights or humanitarian standards from entering areas where there are reasonable grounds to believe that violations of human rights or humanitarian law are being, or have been, committed. Governments may not exclude journalists or representatives of such organizations from areas that are experiencing violence or armed conflict except where their presence would pose a clear risk to the safety of others.

2.2. Exemptions Provisions of the Montenegrin FOI Law

In this section we examine the exemptions provisions of Montenegro's LFATI in the light of the standards set out above.

The exemptions in the LFATI are set out in Article 9, with related provisions being contained in Articles 10, 13 and 14. One of the biggest problems with Article 9 is that it confuses two concepts. One is that it establishes the legitimate interests that may used as a justification for not releasing information if such information would harm ("significantly endanger) these interests – interests such as national security, international relations, public safety, and commercial interests. The second is that it lists the sources or types of information that are deemed to pose harm to such interests.

For example, at Article 9 paragraph 1, reads as follows, stating that information may not be released if it would significantly endanger:

> *national security and defence or international relations, primarily through disclosing the information:*
>
> *a. from security intelligence agencies and intelligence agencies for national security;*
> *b. from military intelligence services;*
> *c. of armed forces activities;*
> *d. about buildings, installations and systems that are intended exclusively for the State defense purposes;*
> *e. of importance for international tribunals or investigation bodies or other international authorities or organizations' work;*

Whilst the protection of national security, defence and international relations are acceptable limitations on the right of access to information in some circumstances, it is completely unacceptable to stipulate that all information whose provenance is the secret intelligence services would necessarily harm one of these interests (eg: would harm national security). Indeed, as a court case in Montenegro has already established, information relating to the budget and some operational activities of the intelligence agencies (the number of people under surveillance in a year) can be released on legitimate grounds of public interest without any harm to state security.

In this respect at least, the limitation under Article 1 benefits from the qualification in the final paragraph of Article 9 which states that:

> *The interests referred to in paragraph 1 of this Article shall be considered significantly endangered if disclosing such information would cause them damages considerably bigger than the public interest in publishing such information is.*

Unfortunately, however, the qualification established by this paragraph does not apply to the other 6 paragraphs of Article 9, which it should (with the possible exemption of paragraph (6) on privacy, although even this may be subject to some limited public interest test, such as when the individual in question is a public figure, when another vital interest is at stake or when the information for other reasons is already accessible in the public domain).

The need to apply the public interest test to other sections of Article 9 can be demonstrated by examination of some of the other paragraphs. For example, paragraph 4.b appears to require that no information held by the government should be disclosed if it relates "to the capital and financial markets" out of an interest in protecting the "economic, monetary and foreign exchange policy of the State". Clearly there is much information that is held by the government that relates to the capital and financial markets that would in no way damage the economic, monetary and foreign exchange policy of the State. In this sense sub-paragraph (b) of Article 9 paragraph 4 is completely superfluous. All that is needed here is to state that information that would cause significant harm to the protected interest (the economic, monetary and foreign exchange policy of the State) may be restricted unless there is an overriding public interest in its release. Both the potential damage and the countervailing public interest should be assessed on a case-by-case basis upon receipt of an actual request for information.

Similarly, while international law permits the restriction of information that would harm "public safety" it is ludicrous to assert that disclosure of information "relating to … the safety of individuals" would necessarily harm public safety (Article 9 paragraph 2.b). Indeed, in many cases, public safety is best protected by the rapid release and widespread dissemination of information related to public safety. For example, advising the public on how to protect themselves in the event of a natural disaster such as an earthquake or how to prevent the spread of an epidemic.

It is evident that the drafters of the Montenegrin LFATI took the language of comparative international standards (such as the Council of Europe Recommendation 2002(2)) and then added a few examples to flesh out the text. This was an unnecessary strategy which unfortunately broadens the exemptions provisions of the law beyond the clearly defined limits of international standards and also creates provisions that will be much harder to interpret in

practice and which are more likely to lead public officials to refuse to disclose information that in fact is completely harmless and that belongs in the public domain.

Of particular concern is the potentially broad interpretation of "business secrets" inserted at Article 9 paragraph 3.b. Whilst private companies do have legitimate business secrets, when they enter into business with the state, such as via a public procurement contract, they must accept that some commercially sensitive information will be released in the interest of guaranteeing transparency and protecting the procurement process from abuse, nepotism and corruption. It will become known, for example, not only the overall price of all bids but, for the winning tender at least, significantly more details about their pricing and operating structure, information that would not normally enter the public domain but which is vital to ensure probity and effective use of the tax-payer's money.

A reworking of Article 9 taking these concerns into consideration might result in language more similar to the following:

Article 9
Access to information may only be restricted if its disclosure would cause serious and irreparable harm to one of the following protected interested and provided that there is no overriding public interest in the disclosure of the information:

1) national security and defence or international relations
2) public safety
3) the legitimate competitive interests of a public or private entity, insofar as this is compatible with the need for public scrutiny of procurement processes;
4) the economic monetary and foreign exchange policy of the State;
5) the prevention, investigation and prosecution of criminal activities;
6) the fair administration of justice;
7) the ability of public authorities to verify compliance with legal requirements through inspections or controls, and to conduct tests or examinations;
8) the confidentiality of deliberations within or between public authorities during the internal preparation of a matter;
9) privacy and other personal rights of individuals.

Information classified under other legislation: It is further unacceptable that Article 9 contains general references to information classified or restricted under other legislation (Article 9, paragraph 3.c refers to information "contained in a separate law on the confidentiality of data). As noted in the international standards section above (Section I), both the OSCE and Council of Europe recommendations require the access to information law takes precedence over any classification of data. In a number of European access to information regimes, information which has been classified will have that classification reviewed upon each and every request for information (in established regimes such as Sweden, for example, this is routinely done by civil servants; in Hungary the Information Commissioner can review classification of information). In no case must the access to information law defer automatically to other legislation: the reason for this is that an access to information is setting out the mechanism for exercise of a fundamental human right and any other legislation that restricts that right cannot automatically

take precedence without at least the right for review of the restriction by the administration and the right to appeal that restriction to an oversight body and eventually to a court of law.

Documents under preparation/Internal Deliberations: Article 9 paragraph 7 confuses two aspects of international standards that permit some limited restriction on access to documents. The first is that documents that relate to, as the Council of Europe defines it "the confidentiality of deliberations within or between public authorities during the internal preparation of a matter" may be exempted from release while such deliberation is ongoing only. This exemption is designed to protect frank expression of opinion during policy debates within government. The second provision woven into Article 9 paragraph 7 is that documents under preparation (or as Article 9, paragraph 7.b puts is "information .. that are in the course of their processing, or the information that are not in any official document form, except for laws or other general documents".

There is a need to disentangle these two notions. With respect to the second concept, that of unfinished documents, while some countries (France, Sweden) register documents as "official" and do not consider documents that have not been registered as falling under the scope of their laws, the majority of countries include all *information* in whatever form as falling under the scope of the law. With the global move towards recognition of the right to information (rather than the earlier and narrower "access to documents" laws) most laws globally do not now exclude *prima facie* any documents or information at all. One survey found that in 18 of the countries surveyed, the definition of information ***includes*** documents under preparation in the sense of unfinished documents. Indeed, in a number of countries it is clearly established in law and practice that they fall under the broad definition of information that is subject to the law. In the UK, for example, the definition of information includes documents under preparation or draft documents[7].

On the other hand, it is quite acceptable to limit for a short period of time while policy-making is going on the exchange of information or opinions that are feeding into the policy development. Once, however, a decision has been made, all related information should be made public. Article 9 paragraph 7 should be reformed to clarify this and to require that when information is related to negotiations or policy formation, it must be made public in due course. When requestors seek such information, they should be informed of when it will become available. In addition, in cases of all such requests, the need to protect policy-making or negotiations should include a public interest test so that in some case the information is made available. An example, would be in the case of an ongoing negotiation relating to privatization of a major state-owned enterprise where there is clearly a significant public interest in the privatization process being as transparent as possible.

Who decides on application of exemptions? A number of access to information laws stipulate that while any officer may release information, restrictions may only be imposed following internal consultations (Mexico's 2002 Federal Law on Transparency and Access to Public Information provides a good model of this, where the information officers may release information but an internal committee has to decide on refusals and be ready to defend such decisions in front of the Information Commission if they are subsequently appealed). It is recommended that the Montenegrin law make clear that while the Information Officer or other public official may release information in accordance with the law, without having to consult with

superiors, only a designated person such as the head of the body may issue a refusal and that person will be personally liable for the refusal decision should it be found to be in breach of the provisions of the law.

What should a refusal notice contain? The LFATI requires that government bodies issue a resolution on whether or not they will release information to a requestor. It is recommended that in the case the decision is to refuse to provide the information, the resolution must contain both the particular provision on which provides the grounds for the information to be withheld (it is not sufficient to cite Article 9 in general) as well as the rationale for the harm it would cause, and a demonstration that the public interest test has been considered. The refusal notice should also inform the requestor of the procedure for appeals (administrative appeal, information commission, courts, etc.) as well as any time frames within which such appeals should be initiated.

Article 10 – Information that may never be restricted

Article 10 is a laudable and welcome provision that establishes which information may never be exempted, even if such information would pose a threat to national security, defence or international relations (Article 9, paragraph 1). It reads:

> *Any government agency shall be in obligation to enable access to the information or to a part thereof, referred to in paragraph 1 of Article 9 of this Law, if such information contains data that obviously imply: disrespect to substantive regulations; unauthorized use of public resources; misuse of powers; unscrupulous performance of public duties; the existence of reasonable suspicions a criminal offence was committed; or the existence of the grounds for attacking a court judgment, regardless of the seriousness of damages caused to the interests referred to in paragraph 1 of Article 9 of this Law.*

This paragraph has the potential to be a powerful tool in work to improve good, efficient and effective governance in Montenegro and to root out corruption. It is not at all clear, however, why this provision applies only to the national security/defence/international relations exemption and not to the remainder of Article 9. This is a similar concern to that identified with the ultimate paragraph of Article 9 (see above). After all there is much information related to questions of public safety, the economic policy of the state, crime prevention, etc., that may also reveal "unscrupulous performance of public duties" and where there would be a significant public interest in obtaining access to such information. There is absolutely no justification for limiting this expanded public interest provision to national security issues.

We further note that other laws that have similar provisions often make reference to the following:

- information on threats or actual harm to the environment
- information that affects the life, health or safety of a person
- information relating to previous, current or potential future violations of human rights

We recommend that these classes of information be added to the list of information that may never be restricted contained in Article 10.

Partial Access Provisions – Article 13

Article 13 establishes the forms of access to information once a request has been granted. It also makes reference to what is known as "partial access" or "severance" which the Article 19 defines accordingly: *"if any part of information is restricted, relevant government agency shall enable access to the information after deleting the part of such information that is restricted."*

Article 13 goes on to specify that if partial access is applied to a document, it shall be indicated with the marking "deletion completed" and an indication of the extent of such a deletion. In cases where there has been a deletion, the only permissible form of access is by a transcript, photocopy or translation delivered to the requestor either in person, by mail or by e-mail.

We recommend that it may be advisable to include a reference to partial access in Article 9 of the law and that Article 9 make clear that where some information in a document would damage a protected interest if released, and if there is no overriding public interest, then the public official **must** provide the requestor with the remainder of the document, after carrying out the appropriate deletions.

Other Grounds for Denial of Information – Article 14

Article 14 provides that government agencies shall not be obliged to provide information that has already been published or made available elsewhere in the country or on the Internet. In such cases the government body shall inform the requestor as to where the information may be found (such as "Official Gazette or other official organ or publication or printed media").

There is a problem with this provision in that it may result in, de facto at least, a requestor not having access to the information and thereby is in effect a denial of the information. Consider for example the requestor who does not have Internet access. Internet Penetration in Montenegro is cited as being 17.6 %, around half the current European average of 38.9%[8]. If this figure is correct, as many as 80% of the population may be denied access to information published on the Internet; even if the true figure is higher or given access to cyber cafes, it is almost certain that around 50% of the population will not have easy Internet access. It is therefore unacceptable simply to refer users to an Internet source without first checking if they have relatively easy access to the Internet.

Similarly, although Montenegro is a small country, not all requestors may have easy access to all the official publications (getting access to a simple information that could be sent on one page by mail may require a full day's journey to the capital Podgorica if a requestor living in a more remote area needs access to a particular official publication not contained in his or her local public library). The principle here should not be simply that the information has previously been published, but that it is genuinely easily accessible for the particular requestor concerned. Part of the duty to assist for each Information Officer referred to in the general analysis section on the LFATI should be to ensure that there the requestor can access the information and if not, to take the decision to provide a copy to him or her.

Article 14 should be reformed to make clear that mere previous publication of information is not sufficient; rather the public official should ensure that the previously published information both (a) answers directly the information request presented by the requestor and (b) is easily available to that particular person.

Recommendations for Reform of Article 9

- It is recommended that Article 9 be reformed to make it clear that all possible grounds for exemptions be subject to both the harm and the public interest tests, ie: that the last paragraph of Article 9 should apply to all preceding paragraphs 1 through 7 (with a possible exemption of some parts of Article 6).
- If maybe appropriate to move Article 9 paragraph 6 to a separate article on protection of privacy and personal data protection, with appropriate references to other data protection provisions when they are introduced in Montenegro (see general analysis of the LFATI).
- It is recommended that Article 9 be amended to remove the language that implies that a particular class of information is exempt from disclosure, or information having a particular provenance or information already classified under some other (unspecified) legislation. In essence Article 9 should consist of a comprehensive enumeration of the permissible protected interests that justify restrictions on access to information along with the mechanism by which such restrictions may be applied.
- Article 9 paragraph 7 should be amended to remove the references to documents under preparation and to clarify that the article is designed to protect internal deliberations and may be applied for limited periods of time (normally a period of a few days or no more than a few weeks).
- Article 9 (or a related Article) should incorporate the requirement that while the Information Officer or other public official may release information in accordance with the law, without having to consult with superiors, only a designated person such as the head of the body may issue a refusal and that person will be personally liable for the refusal decision should it be found to be in breach of the provisions of the law.
- Article 9 (or a related Article) should establish that in the case the decision is to refuse to provide the information, the resolution must contain both the particular provision on which provides the grounds for the information to be withheld (it is not sufficient to cite Article 9 in general) as well as the rationale for the harm it would cause, and a demonstration that the public interest test has been considered. The refusal notice should also inform the requestor of the procedure for appeals (administrative appeal, information commission, courts, etc.) as well as any time frames within which such appeals should be initiated.

Recommendation on Article 9 / Article 13

- We recommend that it may be advisable to include a reference to partial access in Article 9 of the law and that Article 9 make clear that where some information in a document would damage a protected interest if released, and if there is no overriding public interest, then the public official **must** provide the requestor with the remainder of the document, after carrying out the appropriate deletions.

Recommendation on Article 10

- We recommend additional classes of information (environment, life, health and safety, and human rights violations) be added to the list of information that may never be restricted contained in Article 10.

Recommendation on Article 14

- Article 14 should be reformed to make clear that mere previous publication of information is not sufficient; rather the public official should ensure that the previously published information both (a) answers directly the information request presented by the requestor and (b) is easily available to that particular person.

2.3. The Nature and Structure of State Secrets Laws

Montenegro is on the point of adopting a state secrets law. It should be very clear therefore on the purposes of such a law. The primary aim of a state secrets law is to ensure that information that will cause harm to national interests (national security, territorial integrity, international relations, public safety) is protected in such a way that it does not fall into the wrong hands.

The volume of information that should be protected by a state secrets law should be a tiny percentage of all the information held by government. There are two reasons for this. One is that the majority of information held by government will not cause serious harm to the national interests. In a modern democratic society all information that does not absolutely need to be kept secret should be automatically in the public domain. The second reason is that it is very hard to ensure that the real damaging information is kept secret if all information is liberally classified as "top secret" or "classified" – in such a case it becomes impossible to distinguish between the really harmful information and that which is actually quite benign.

There is also a cost to keeping information secret: it requires special handling procedures, should be kept in secure locations, put in the safe or other secure storage overnight, only processed and read by those who have the appropriate level of security clearance. If a large volume of information has to be treated in such a way there are two possible outcomes: the first is that the information will not be properly handled and the risks of it falling into the wrong hands increase significantly. The second is that it is properly handled but that the cost of such and operation escalates dramatically.

It is for this reason that the NATO document cited in Section I states:

> *"the classification assigned determines the physical security given to the information in storage and transmission, its circulation, destruction and the personnel security clearance required for access. Therefore both over-classification and under-classification should be avoided in the interests of effective security as well as efficiency."*[9]

These are also some of the reasons that the OSCE in its recommendations cited in Section I above states:

> *"The definition of state secrets should be limited only to data that directly relate to the national security of the state and where their unauthorized release would have identifiable and serious consequences. Information designated as "Official" or "work secrets" should not be considered for classification as state secrets."*

The purpose of a state secrets law should be, therefore, to establish the procedures for classifying information in order to ensure that information that genuinely needs to be limited in circulation is properly marked and handled.

A typical state secrets law will include the following elements:

- definition of the levels of classification, which are typically: Top Secret, Secret, Confidential, and Restricted (not forgetting the 5th category of unclassified which does not need to be marked on all documents as it is presumed if the document is not otherwise classified).
- procedures for applying the classification – including who proposes and who approves the classification of a document, the issuance of "security certificates" or other authorization to confirm the classification.

- procedures for applying classification to a document containing more than one level of secret
- rules for applying time limits to the classification (and automatic declassification)
- rules on the periodic review of classification
- the procedures for handling and protecting classified, ensuring it is protected from unauthorized disclosure. The management procedures will include how such information is identified, controlled, transferred, transmitted, retrieved, indexed, archived, and/or eventually destroyed. Such procedures include how to ensure the physical security of locations where classified information is held in order to prevent access by unauthorized persons.
- particular measures that related to the handling of classified information that is held in electronic form and therefore requires particular resources for its storage, transmission, processing, use, and sharing. The security of the information systems will involve special protection against unauthorized access to or modification of the classified information. There will need to be special considerations given to the protection of related computer hardware and software.
- the procedures for issuing security clearance to personnel who will handle classified information. This can be complex because different levels of classification imply different levels of security clearance; whilst a small number of people may have access to a top secret document, a larger number may have access to one that is confidential or restricted. The state secrets law will also give consideration to the automatic security clearance of those elected to high government office.
- creation of an oversight body, which as the OSCE recommends should be "an independent body that is not part of the intelligence, military or security services should have oversight over classified information and ensure that the system is operating properly, receive complaints about improperly classified information and review and order the declassification of information."

A good state secrets law will complement and in no way contradict an access to information law. The state secrets law merely identifies the procedures for handling and protecting information that has been identified as potentially damaging to the national security interest. An access to information law on the other hand regulates the right of access to information. In a well functioning democratic system, it is relatively rare that a request for information actually seeks access to information that, properly classified, is marked as "top secret" or "secret". For example, requestors do not normally seek to know the details of the current system for codifying sensitive messages used within the military. Hence, where information classification is properly applied, it will be very clear which information should and should not enter the public domain. There will however be occasions when a requestor seeks information that has been classified. This might be because the requestor believes that there is a public interest in knowing the information or (as is often the case) the classification has been made for political rather than security reasons. In such cases it is imperative that the request for information be given due consideration under the access to information law and that the requestor has a right to appeal any refusal to higher bodies and eventually to the courts. No information should automatically be excluded from consideration under the access to information law merely because it has been classified according to the state secrets law.

2.4. Protection of Commercial Interests and Business Secrets

The aim of protecting commercial interests is to ensure that there is a level playing field and that businesses can maintain a fair competitive advantage based on their investment of skill, research, and resources into developing and marketing their products.

The Council of Europe Recommendation establishes an exemption for "commercial and other economic interests", and explains these as, "for example business matters which need to be kept secret for competition reasons, such as the confidential nature of business negotiations."

Generally speaking, commercial interests is a broader term than trade secrets which are closely guarded secrets giving significant competitive edge, such as the secret formula for Coca Cola. Definition of these concepts becomes rather difficult when trying to compare between legal regimes, because of nuances of difference between different regimes, but it is clear that a "trade" or "business" secret is a much narrower concept than "commercial interests". Often "trade secrets" will be subject to a legal regime that requires them to be registered in order to be able to enforce subsequent legal protection, as with patents and trademarks and other forms of copyright.

What is also clear is that not all information which gives companies a competitive advantage should remain out of the public domain. Most businesses have to file some form of annual report and accounts and some of this information is in the public domain in the majority of countries, with a significantly larger amount of information being available to shareholders and hence the public for publicly-listed companies (companies listed on the stock exchange in any particular country).

A wide range of other information about private businesses routinely enters the public domain. For example, if it is found that a company that manufactures consumer electronic products (televisions or refrigerators for example) has been seriously and repeatedly polluting the environment, this information could hurt the reputation and therefore the sales of the company, but this is evident that the public that has the right to the information and to make choices based on being fully informed.

Similarly, in the USA, the local newspapers regularly carry information about which kitchens have been fined the previous month for failing health inspections of their kitchens. Such information will almost inevitably lead to a decline of customers going to the restaurant, thereby hurting the business, but it is also evident why the information should enter the public domain.

In Argentina, a 2004 nightclub fire in which 175 people died and over 700 were injured, many of them seriously, caused a scandal when it became clear that the venue did not have the licence for a large-scale event and was not following fire-procedures correctly. As a reaction, people started filing access to information requests with other venues to gather information about the nature of the licences they had obtained, actions which gave a boost to the campaign for a full access to information law.

Nevertheless, a great deal of information about the functioning, financial and personnel structures of private companies will remain private under normal circumstances. This changes radically when a company enters into a financial relationship with a public body, such as with a public procurement contract.

The principle here is the same as when a public official enters office: while a private individual has the right to keep secret certain information such as about their assets, income, business dealings, etc., confidential, someone who puts themselves forward for public office cannot expect the same level of privacy. So, for example, holders of public office and more senior public official have to declare their assets and interests.

This holds too for private companies that when they enter into a relationship with public bodies and receive public funds, must expect that there is some level of scrutiny. This scrutiny is justified because in these cases the balance between the commercial confidentiality interests of the company are outweighed by the public interest in transparency in the spending of public funds.

Commercial interests vs. public procurement transparency

Emerging standards indicate that the limits of commercial confidentiality are significantly narrower when a private company does business with government. In addition to the law and practice in many European Countries, a number of important cases by Information Commissioners have ruled that commercial information should be released in the interest of transparency of a public procurement contract and to enable the public to know how its funds are being spent.

Irish Case on Pricing Structures in Contracts

In 2003, the Irish freedom of information commissioner ruled that information in contracts between the government and private companies could be made public, even if it had the potential to damage the competitive edge of that company.[10]

The case arose from a request filed under Ireland's 1997 Freedom of Information Act for a contract between Ireland's Department of Finance and financial advisors, ABN Amro and McCann FitzGerald Solicitors, that amounted to €850,247, which the commissioner noted was a "large amount of public money."

The total amounts paid had already been made available by the minister of finance (see Table 5), but the requestors wanted details of the contract. The financial advisors objected to the contract being made public because it would reveal their fee and pricing structure which, they claimed, would give competitors an advantage.

The Irish information commissioner ruled that once the contract had been signed, "The successful tender information lost confidentiality with respect to the fee rates and other details necessary to understand the nature of the services contracted for." He concluded that this was

true, even if harmful to the competitive position of the affected parties: "On balance, the public interest was better served by the release of this information in light of the significant need for openness and accountability in relation to the contract."

Slovenian Case on Access to Contracts

In another precedent-setting case, the Slovenian information commissioner confirmed that procurement contracts between public bodies and private suppliers are public information, except where trade secrets that give a competitive advantage are concerned.[11] The case resulted from an information request filed on February 22, 2004 by a member of the public who asked for a copy of the agreement between the municipality and a private company, ALPDOM Inženiring, for management of apartments blocks owned by the municipality.

The Municpality of Radovljica rejected the request on the grounds that it was confidential under Slovenia's 1993 Companies Act. The municipality also cited Article 6 of Slovenia's Access to Information Act, which provides for protection of trade secrets.

The requestor appealed, arguing that the agreement had to be freely available, to allow public participation in the decisions relating to the management of publicly-owned housing. A supplementary concern was that a manager of ALPDOM Inženiring was also the deputy-mayor of the local municipality, hence there was a clear intermingling of public and private interests.

The information commissioner ruled that the contract should be released.

The Slovenian Information Commissioner's Principles

The Slovenian Information commissioner citied a number of grounds that reflect comparative standards for public procurement contract transparency:

- information in a contract that does not impact on the competitive market position of the selected provider cannot be considered a trade secret;
- data cannot be defined as a trade secret if other laws require it to be public (in this case the Slovenian Public Procurement Act of 2000);
- data cannot be defined as a trade secret if it relates to violations of law or breaches of good business practices;
- an entire contract cannot be considered a trade secret as part of the information contained in a contract has to be made public during the bidding process;
- the total financial value of the contract cannot be reserved;
- the object of the tender & description of services/goods to be supplied cannot be reserved;
- supporting references must be made public, as they relate to compliance with the procurement conditions and criteria;
- assessment of eligibility and compliance criteria cannot be reserved, as these are an essential component of awarding a public contract, and the public has the right to know whether the selection procedure has been carried out correctly and whether the selected bidder made the best possible offer.

The information commissioner also noted that, in addition to the above considerations, information may only be considered a trade secret if it has been specified as such by the supplier and if it does not relate directly to the procurement at issue. The commissioner recommended that, if bidders declare large parts of the information they submit to be trade secrets, the contracting agency should exclude the bids. Where contracts contain some genuine trade secrets, the information must be severed, either physically removed or crossed out, or electronically deleted in a password-protected form in order to permit the remainder of the information to be released.

UK Standards on Private and Public Commercial Interests

A similar principle applies in the UK. The guidance issued by the Information Commissioner's Office in Freedom of Information Awareness Guidance No. 2 reinforces the advice given by the Lord Chancellor's on the handling of information requests:

> *When entering into contracts public authorities should refuse to include contractual terms which purport to restrict the disclosure of information held by the authority and relating to the contract beyond the restrictions permitted by the Act. Public authorities cannot "contract out" of their obligations under the Act. Unless an exemption provided for under the Act is applicable in relation to any particular information, a public authority will be obliged to disclose that information in response to a request, regardless of the terms of any contract.*

In some cases, the public authority itself may claim that it has commercial interests to protect. This arose in a case in the UK when a public body (a publicly funded art gallery the National Maritime Museum, refused to reveal the amount of money it was paying to artists exhibiting at the museum, saying that this would damage its negotiating position with other artists. The UK's Information Tribunal (a court which hears appeals against decisions of the Information Commissioner) ruled that the given that each case and each negotiation is likely to be slightly different the risk cannot be assumed to exist and stated: "We have accordingly concluded that no sufficient risk of prejudices to the commercial interests of National Maritime Museum was demonstrated to justify the exemption". There was clearly an overriding public interest in knowing how the public funds were spent and how much the artists were receiving for their shows.

Montenegro's Exemptions on Commercial Confidentiality

Article 9 of Montenegro's LFATI at paragraph 3 states that information may be refused if it would cause significant harm to:

> *4) commercial and other private or public economic benefits, through disclosing the information:*
>
> *a. relating to financial, monetary or commercial operations of the State with other states, international organizations or other legal or natural entities;*
>
> *b. that are business secrets;*
>
> *c. contained in a separate law on the confidentiality of data;*

The first clause of Article 9 paragraph 3 is in line with the standards of the Council of Europe and with Regulation 1049 Regulation 1049/2001 on access to EU documents which permits exemptions in order to protect the "*commercial interests of a natural or legal person … unless there is an overriding public interest in disclosure* (Art. 4)."

However, as with other articles in the exemptions section of Montenegro's law, the additional clauses are somewhat problematic. Sub-paragraph 3(a) seems to confuse the traditional concept of commercial interests with that the State's financial or monetary policy and with international relations. It is an unnecessary duplication and confusion of the initial clause of Paragraph 3 and should be deleted.

Sub-paragraph 3(b) is legitimate as a mention assuming that (a) business secrets in the term of trade secrets (the formula for Coca Cola) are clearly and narrowly defined in Montenegrin law and that each request for information takes into consideration the public interest in the information as set out above. In particular, it should be clear the difference between "business secrets" in private business operations and the need to disclose information when a business enters into a contract with the government. In order for this to be achieved, the public interest text needs to be extended to apply to Paragraph 3 as we have already recommended in Section II above.

Sub-paragraph 3.c is highly problematic. It makes a general reference to another law. It is not clear to use if this legislation currently exists. In any case, as argued in Section II above, the LFATI cannot make a blanket deferral to another law. Certain types of confidentiality may be protected (lawyer-client privilege for example) but that should be included as one of the protected interests under this law and subject to the public interest test.

Recommendations

- To bring Article 9 paragraph 3 into line with the Council of Europe standards, all but the first clause should be deleted.
- If it does not yet have one, Montenegro needs a well-drafted law on trade or business secrets.

Information about the Author

Helen Darbishire, Executive Director of Access Info Europe, is a human rights professional specializing in access to information, freedom of expression and media freedom. She has worked on the drafting and implementation of numerous access to information laws in Europe, Latin America, and Africa, and was one of the experts commissioned by the OSCE to draft the Bosnian FOI law. She has also worked on the analysis of media, broadcasting, state secrets and data protection legislation.

Ms Darbishire has directed numerous projects designed to promote use of and respect for the right to information, with project work including training of civil society and public officials, provision of technical assistance to government bodies, and the design and implementation of monitoring studies to evaluate compliance with the access to information legislation. She has been closely engaged in litigation to defend the right to information, including through contributions to amicus briefs in international court cases, and has provided expert contributions to the treaty on access to official documents currently being drafted by the Council of Europe.

In 2005, Helen Darbishire helped found and became the first director of Access Info Europe. Helen is also a founder member and current chair of the Freedom of Information Advocates Network.

Ms Darbishire's human rights experience spans 17 years, working first with Article 19 based in London and Paris (1989-1998), and then with the Open Society Institute based in Budapest and New York (1999-2005), as well as being a consultant for inter-governmental organizations (including UNESCO and the Council of Europe) and a number of non-governmental organizations. She has published and lectured widely on freedom of expression and democratization issues. She holds a degree in History and Philosophy of Science and Psychology from the University of Durham, UK.

Helen is based in Madrid, Spain

Access Info Europe

Calle Príncipe de Anglona 5, 2o centro
28005 Madrid, Spain
e-mail: info@access-info.org
www.access-info.org